

Symantec™ Clientless VPN Gateway 4400 Series Installation Guide

Supported Platforms:

Models 4420 and 4460



Symantec™ Clientless VPN Gateway Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 1.0

PN: 10-20-09294

January 30, 2004

Copyright notice

Copyright © 1998–2004 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide

Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/techsupp/ent/enterprise.html, select licensing and Registration, then select the product and version that you wish to register.

Contacting Technical Support

Customers with a current maintenance agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp/.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information

- Problem description
- Error messages/log files
- Troubleshooting performed prior to contacting Symantec
- Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com/techsupp/, select the appropriate Global Site for your country, then select the enterprise Continue link. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1	Introducing Symantec Clientless VPN Gateway 4400 Series	
	About the Symantec Clientless VPN Gateway 4400 Series	5
	Intended audience	6
	Document structure	6
	About product documentation	7
	Checking the components list	7
	Replacement CD-ROMs	8
Chapter 2	Installing the appliance	
	Planning for installation	9
	Installing your free-standing appliance	9
	Mounting in a rack	10
	About model 4420	11
	Connecting model 4420 to the network	12
	Connecting power cord to model 4420	13
	Turning on the power for model 4420	13
	About model 4460	13
	Connecting model 4460 to the network	14
	Connecting the power cord to models 4460	14
	Turning on the power for the model 4460	15
Chapter 3	Appliance setup and initial system configuration	
	Before you begin initial setup	17
	Front panel layout	19
	Front panel controls	20
	Example network diagram	22
	Using the network setup worksheet	23
	Network setup worksheet	23
	Changing passwords	24
	Performing the initial appliance network setup	24
	Displaying system information	26
	Using the system menu	27
	About the Security Gateway Management Interface	27
	Connecting to the appliance	28
	Configuring your Clientless VPN Gateway appliance	29

Locking front LCD panel controls	29
Unlocking the front LCD panel controls	29
Using the command-line interface (CLI)	29
Running the Quickstart Wizard (Optional)	30
Command-Line Interface (CLI) features	32
Uniform command formats	33
Auto-complete	33
Auto-list	33
Configuring the Ethernet port	33
Adding the default gateway	35
Restoring the software	36

Chapter 4 License setup

About license files and licensing	39
Getting started with your 30-day grace period	39
Obtaining and organizing license serial numbers	40
Gather your Serial Number Certificates	40
Sort your serial numbers for each appliance	40
Collect product and contact information	40
Plan for your license file	41
Obtaining your license file	42
Organizing your license files	42
Using the Symantec License Request & Maintenance Web site	44
Activating your license files	44
Uploading your license files	50
Removing license files	51
Explanation of the appliance licensing and maintenance	51
Obtaining a license file	51
Basic license types	51
Maintenance contracts	52
Maintenance renewals	53
Platinum support uplift	53
High availability license bundles	53
Load balancing license bundles	53
About Symantec Clientless VPN Gateway 4400 Series licenses	53

Appendix A Developing a pre-installation security plan

About developing a security plan	56
Defining your security policy	56
Before writing your security plan	57
Becoming security-conscious	57
Educating users	58

Involving the user community	58
Filling out worksheets	59
Defining your organization	59
Site hardware information	61
TCP/IP address	62
Allowed TCP/IP services	64
Web service information	65
Defining your network architecture	68

Appendix B Legal agreements

About the Symantec Clientless VPN Gateway 4400 Series licenses	71
SYMANTEC CLIENTLESS VPN GATEWAY APPLIANCE LICENSE AND WARRANTY AGREEMENT	71
1. Software License:	72
2. Content Updates:	73
3. Limited Warranty:	73
4. Disclaimer of Damages:	75
5. U.S. Government Restricted Rights:	75
6. Export Regulation:	76
7. General:	76
8. Excluded Software:	77
Third-party attributions	77
A. Apache Software License, v 1.1	77
B. Mod_SSL Package License	77
C. OpenSSL Library License	77
D. SSLeay License	77
E. The PHP license version 3.0	77
F. Q Public License, Version 1.0	78
G. Berkeley DB Software Copyrights, Conditions, and Disclaimers	78
H. Libpng Library Requirements, Copyright, and Disclaimer	78
I. Linux Loader Requirements, Copyright, and Disclaimer	78
J. OpenLDAP Public License Version 2.7	78
K. SSH Implementation Requirements, Copyrights, and Disclaimers	78
L. Zlib Requirements, Copyright, and Disclaimer	78
M. Popt Requirements, Copyright, and Disclaimer	79
N. Pam Requirements, Copyright, and Disclaimer	79
O. Inetd Requirements, Copyright, and Disclaimer	79
P. Ncurses Requirements, Copyright, and Disclaimer	79
Q. Graphviz License Agreement Version 1.2D	79
R. VRRPD License Terms	80
S. GNU Free Documentation License Version 1.2 Copyright (C) 2000,2001,2002 Free Software Foundation, Inc.	80
GNU library general public license	80

Appendix C	Troubleshooting	
	About troubleshooting	86
	Accessing troubleshooting information	86
Appendix D	Specifications and safety	
	About this appendix	88
	Product specifications	88
	Safeguard instructions	89
	Product certifications	91

Introducing Symantec Clientless VPN Gateway 4400 Series

This chapter includes the following topics:

- [About the Symantec Clientless VPN Gateway 4400 Series](#)
- [Intended audience](#)
- [Document structure](#)
- [About product documentation](#)
- [Checking the components list](#)

About the Symantec Clientless VPN Gateway 4400 Series

The Symantec Clientless VPN Gateway is a Secure Sockets Layer (SSL) based dedicated appliance that provides the complete security essential for enabling universal enterprise remote access.

The Symantec Clientless VPN Gateway 4400 Series supports the following end user clients (Internet browsers).

Table 1-1 User access browser support

Platform	Browser
Windows	Internet Explorer v5.5 or later

Table 1-1 User access browser support (Continued)

Platform	Browser
Linux	Mozilla 1.5, and Netscape v4.5 or later
Mac	Internet Explorer v5.5 or later
Windows Mobile 2003	Internet Explorer
Palm v5.x	Web Pro v3.0
Unix	Netscape v7.x

You can use Microsoft Internet Explorer version 6 or later or Netscape Navigator version 7 or later to manage your Symantec Clientless VPN Gateway 4400 Series through the Security Gateway Management Interface (SGMI). In addition, you must ensure that your SGMI workstation has a minimum of 512 MB of RAM.

Intended audience

This manual is intended for system managers or administrators responsible for administering the Symantec Clientless VPN Gateway 4400 Series.

Document structure

This manual is structured as follows:

Table 1-2 Document structure

Chapter	Title	Content
Chapter 2	Installing the appliance	Tells you how to do a stand-alone or rack mount install of the Symantec Clientless VPN Gateway 4400 Series.
Chapter 3	Appliance setup and initial system configuration	Tells you how to initially set up the appliance and run the Quickstart Wizard.
Chapter 4	License Setup	Tells you how to obtain and upload your license file.
Appendix A	Developing a pre-installation security plan	Lays out basic guidelines for developing an overall security plan and provides a checklist for assessing your security issues.

Table 1-2 Document structure (Continued)

Chapter	Title	Content
Appendix B	Legal agreements	Lists all Symantec product legal agreements.
Appendix C	Troubleshooting	Tells you where to find troubleshooting information.
Appendix D	Specifications and safety	Lists the product specifications and the certifications obtained for the appliance.

About product documentation

The Symantec Clientless VPN Gateway 4400 Series functionality is described in this guide and the *Symantec™ Clientless VPN Gateway 4400 Series Administrator's Guide*.

The *Symantec™ Clientless VPN Gateway 4400 Series Administrator's Guide* describes the SGMI and covers topics related to the Symantec Clientless VPN Gateway 4400 Series and its related components including: concepts, deployment scenarios, administration tasks, configuring the server, managing users and access profiles, authentication schemes, roles, Uniform Resource Locator, configuring access profiles, configuring user portal pages, configuring end point clients, maintaining the server and the user interface. It is provided in PDF format.

Checking the components list

After carefully unpacking the Symantec Clientless VPN Gateway 4400 Series appliance, compare the kit contents with [Table 1-3](#) to ensure that you have received all ordered components.

Table 1-3 Components list

Part	Description
Appliance	A single device.
Rack-mount brackets	Hardware for rack-mounting the appliance. Screws for attaching the bracket to the appliance are included; however, screws for attaching appliance to the rack are not included.

Table 1-3 Components list (Continued)

Part	Description
<i>Symantec Clientless VPN Gateway v5.0 Software and Documentation for 4400 Series</i> (the restore CD-ROM)	<div>Contains the following items:</div> <ul style="list-style-type: none">■ Appliance restore partition■ Adobe Acrobat Reader <div>All documentation for this product is provided in PDF format. Printed documents are noted.</div> <ul style="list-style-type: none">■ <i>Symantec™ Clientless VPN Gateway 4400 Series Installation Guide</i> (also printed).■ <i>Symantec™ Clientless VPN Gateway 4400 Series Administrator's Guide</i>■ <i>Symantec™ Clientless VPN Gateway 4400 Series Quick Start Cards for the 4420 and 4460</i> (also printed).■ <i>Symantec™ Clientless VPN Gateway 4400 Series Release Notes</i> (also printed).
Cables	<ul style="list-style-type: none">■ A power cord appropriate for the country in which the appliance will operate■ Network crossover cable■ Null modem serial port cable

Replacement CD-ROMs

You may need to replace the media due to a defective or lost CD-ROM. If you need a replacement CD-ROM because it is defective, contact Customer Support.

If you require a new CD-ROM because you have lost it, contact your Sales Representative to purchase a new media kit.

Installing the appliance

This chapter includes the following topics:

- [Planning for installation](#)
- [About model 4420](#)
- [About model 4460](#)

Warning: This is an electrically powered device. You must adhere to warnings when installing or working with the Symantec Clientless VPN Gateway 4400 Series.

Planning for installation

This chapter contains information about installing the appliance, connecting it to the network, and turning on the power. Before you start you should have a pre-installation security plan. See “[Developing a pre-installation security plan](#)” on page 55.

Note: Read the installation instructions before connecting the system to its power source.

You can install the Symantec Clientless VPN Gateway 4400 Series either free-standing or in a rack.

Installing your free-standing appliance

You can install the Symantec Clientless VPN Gateway 4400 Series as a free-standing appliance.

To install the free-standing appliance

- 1 Ensure that the installation site has a smooth and level surface, such as the top of a computer table in a minimum access area. In addition, avoid placing the Symantec Clientless VPN Gateway 4400 Series appliance in a cluttered or busy area. Ensure this area is only accessible by authorized security personnel. The installation site must meet minimum product specifications.

Note: Ensure that location for the front and rear of the appliance is free of debris to provide sufficient air flow.

- 2 Ensure that the power source is adequate and that the outlet is located within reach of the supplied power cord without stretching or putting strain on the cord.

Warning: Do not use an extension cord to supply power to this unit.

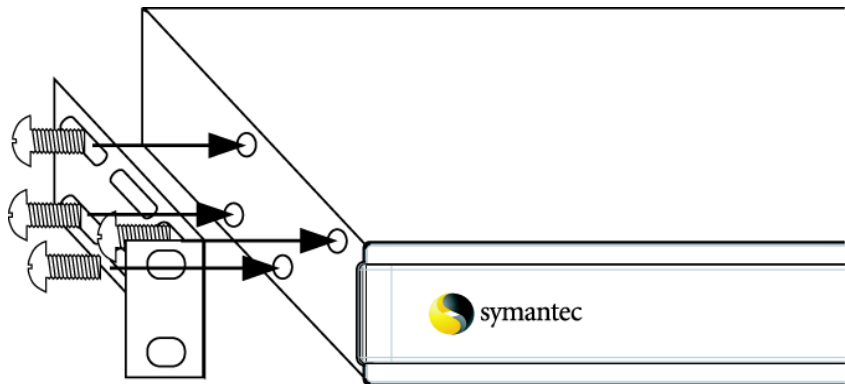
- 3 After cabling the unit into the network, position the cables away from foot traffic.

Mounting in a rack

The following rack-mounting instructions apply to all appliance models.

To mount the appliance in a standard 19-inch equipment rack

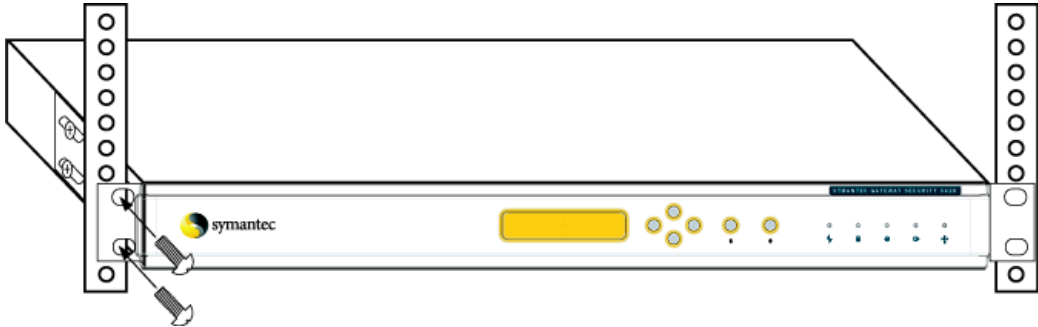
- 1 Connect the mounting brackets to the sides of the appliance using the supplied bracket screws.



Because rack hardware can differ from site to site, rack-mounting screws are not shipped with the unit. Screws for attaching the bracket to the appliance

are included. Before installing your appliance, obtain the proper size screws for mounting the appliance in your specific rack.

- 2 Connect the mounting brackets to the sides of the appliance towards the front or the rear of the case.



- 3 Secure the mounting brackets to the equipment rack.

About model 4420

This section describes the back panel of the Symantec Clientless VPN Gateway model 4420. Model 4420 offers two active 10/100 Fast Ethernet ports. There are four inactive ports for future expansion.

[Figure 2-1](#) shows the location back panel features for model 4420.

Figure 2-1 Model 4420 back panel

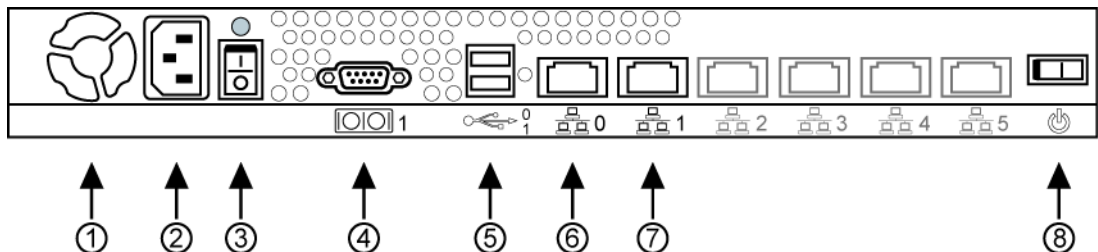


Table 2-1 describes the back panel of model 4420.

Table 2-1 Model 4 420 back panel feature

Location	Feature	Description
1	Cooling fans	Maintains proper operating temperature. Ensure that the ventilation holes in the front and back are not blocked.
2	Power socket	Connection for AC power cord.
3 (top)	Power indicator	Shows if unit is turned on.
3 (bottom)	Master power switch	Turns the appliance on or off.
4	Serial console port (115200 bps)	Lets you connect a terminal emulator to act as a system console and lets you log on to the system console and access the Command-line Interface (CLI).
5	USB ports	USB ports are not currently supported.
6	int0	Accepts a 10/100Base-T network cable, which enables Ethernet network connection.
7	int1	Accepts a 10/100Base-T network cable, which enables Ethernet network connection.
8	Power reset switch	Resets appliance.

Connecting model 4420 to the network

The Clientless VPN Gateway model 4420 back panel provides a total of two usable Fast Ethernet connections. Your network connection requirements may differ depending on your site’s configuration. Use the location numbers from [Figure 2-1](#) to refer to the back panel mentioned in each step.

To connect your network

- 1 Plug the RJ-45 connector from the local area network (LAN) into int0 the inside network connection (6). For initial setup, this must be a directly connected LAN.
- 2 Plug the RJ-45 connector from the Internet into int1the outside network connection (7).

Connecting power cord to model 4420

Use the location numbers from [Figure 2-1](#) to refer to the back panel mentioned in each step.

To connect power to the appliance model 4420

- 1 Plug the power cord into the power socket on the rear panel (2).
- 2 Connect the power supply cord from the appliance to an electrical outlet or UPS supply unit.

Turning on the power for model 4420

Turn on the power by pressing the master power switch (3) on the back of the Symantec Clientless VPN Gateway 4400 Series. See [“Connecting model 4420 to the network”](#) on page 12. The appliance has powered up properly when the following things happen:

- The hard disk spins, the fans turn on, and the LEDs and LCD screen on the appliance light up.
- A number of status messages and Symantec CVG 5.0 display on the LCD screen when the appliance completes its start process.

About model 4460

This section describes the back panel features of the Clientless VPN Gateway model 4460. Model 4460 offers two 10/100/1000 Gigabit Ethernet ports. There are four inactive ports for future expansion. Refer to [Figure 2-2](#) for a back panel view of the 4460.

Figure 2-2 Models 4460 back panel

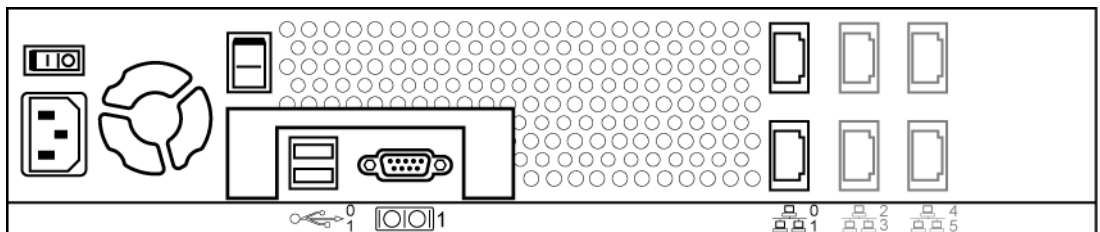


Table 2-2 lists the model 4460 back panel.

Table 2-2 Model 4460 back panel

Location	Feature	Description
1 (top)	Master power switch	Turns the appliance on or off.
1 (bottom)	Power socket	Connection for AC power cord.
2	Cooling fan	Maintains proper operating temperature. Ensure that the ventilation holes in the front and back are not blocked.
3	Power reset switch	Resets appliance.
4	USB ports	The USB ports are currently unsupported.
5	Serial console port (115200 bps)	Lets you connect a terminal emulator to act as a system console and lets you log on to the system console and access the Command-line Interface (CLI).
6	int0 (top) and int1(bottom)	Accepts a 10/100Base-T network cable, which enables Ethernet network connection. int0 is the inside interface and int1 is the outside interface.

Connecting model 4460 to the network

The Clientless VPN Gateway model 4460 offers two usable gigabit Ethernet connections. You must configure the inside and outside interfaces as int0 and int1 respectively.

To connect models 4460 to the network

- 1 Plug the RJ-45 connector from the LAN into the inside interface int0 network connection (6 top).
- 2 Plug the RJ-45 connector from the Internet into the outside interface int1 network connection (6 bottom).

Connecting the power cord to models 4460

The following procedure describes how to connect the power cord. Use the location numbers from Figure 2-2 to refer to the back panel mentioned in each step.

To connect power to appliance models 4460

- 1** Plug the power supply cord into the power socket on the rear panel (1 bottom).
- 2** Connect the power supply cord from the appliance to an electrical outlet or UPS supply unit.

Turning on the power for the model 4460

Turn on the power by pressing the master power switch (1 top) on the back of the Clientless VPN Gateway appliance model 4460. The appliance has powered up properly when the following things happen:

- The hard disk spins up, the fans turn on, and the LEDs and LCD screen on the appliance light up.
- A number of status messages and Symantec CVG 5.0 display on the LCD screen when the appliance completes its start process.

Appliance setup and initial system configuration

This chapter includes the following topics:

- [Before you begin initial setup](#)
- [Front panel layout](#)
- [Example network diagram](#)
- [Using the network setup worksheet](#)
- [Performing the initial appliance network setup](#)
- [Displaying system information](#)
- [Using the system menu](#)
- [About the Security Gateway Management Interface](#)
- [Connecting to the appliance](#)
- [Configuring your Clientless VPN Gateway appliance](#)
- [Restoring the software](#)

Before you begin initial setup

This chapter describes the initial set up and LCD configuration of the Clientless VPN Gateway appliance, which includes getting the appliance set up and running. For information on configuring the appliance through the GUI, see the *Symantec Clientless VPN Gateway 4400 Series Administrator's Guide*.

There are two steps to take before beginning the initial setup process:

- Develop a security plan.

See “[Developing a pre-installation security plan](#)” on page 51.

- Complete the appliance installation process described in Chapter 2.

Developing a security plan is the most important piece of your installation process. Appendix A provides worksheets for developing your security policy and a checklist for gathering the information you need to facilitate the installation process.

During this process, gather the required IP addresses that will make your installation process a success. Initially, you need the IP address and netmask of the Clientless VPN Gateway network interface through which the appliance will be managed.

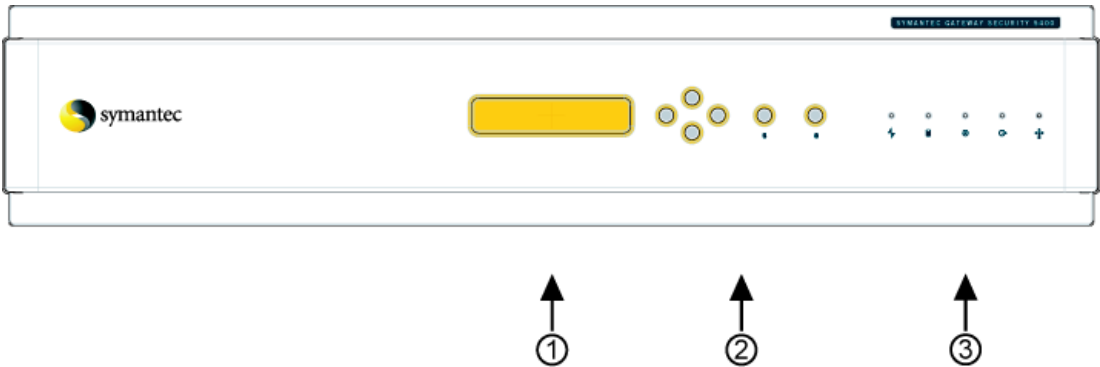
You can use the Clientless VPN Gateway appliance without a license file for a 30-day evaluation period. At any point during those 30 days, use the online license file generator from the Symantec licensing and registration Web site at <https://licensing.symantec.com> to obtain license files. See “[Using the Symantec License Request & Maintenance Web site](#)” on page 74.

Once you have developed your security plan and completed the preliminaries, you are ready to set up your Clientless VPN Gateway. The setup takes approximately 15 minutes, if you have the IP address information in hand.

Front panel layout

The Clientless VPN Gateway front panel, shown in [Figure 3-1](#), contains six data entry and navigation buttons, a two-line by 16 character liquid crystal display (LCD) area, and status indicators. The front panel looks the same on all models, except the 4420 has a narrower profile. The initial setup of the Clientless VPN Gateway appliance takes place at the appliance’s front panel, where you enter and modify parameters, such as system and network IP addresses.

Figure 3-1 Symantec Clientless VPN Gateway 4400 Series front panel








[Table 3-1](#) describes the elements of the front panel and how they work.

Table 3-1 Front panel descriptions

Location	Feature	Description
1	LCD	<div>Displays the Clientless VPN Gateway software version number and system monitoring information.</div> <div>You can monitor appliance status, modify configuration parameters, and reinitialize the appliance. The available LCD screen includes:</div> <div><ul style="list-style-type: none">■ System startup self-tests■ Performance monitoring■ System menu. See “Using the system menu” on page 27.</div>
2	Front panel controls	<div>Lets you enter network information directly into the appliance. See “Front panel controls” on page 20.</div>

Table 3-1 Front panel descriptions (Continued)

Location	Feature	Description
3	Status indicators:	
		The outside network activity indicator blinks when there is traffic on the outside network interface (int1) of the model 4420. This feature is disabled on the model 4460.
		The inside network activity indicator blinks when there is traffic on the inside network interface (int1) of the model 4420. This feature is disabled on the model 4460.
		The power indicator glows steadily to indicate the power is on.
		The disk activity indicator blinks when there is activity on the hard disk drive.
		The temperature indicator blinks to indicate temperature status. It blinks slowly for temperature warnings and quickly for temperature failures. If the appliance is in danger of overheating, a log message is sent to the appliance log file.

Front panel controls

The front panel controls are the same on all models. Use these instructions to enter all required setup information into the Clientless VPN Gateway appliance. See [“Performing the initial appliance network setup”](#) on page 24.

The front panel controls perform dual functions. These functions depend upon whether the Clientless VPN Gateway appliance is in initial setup mode or if you are using the system menu. Refer to the descriptions below. The front panel controls consist of four navigation buttons, a select (s) button, and an enter (e) button. [Figure 3-2](#) shows the front panel controls.

Figure 3-2 Front panel controls

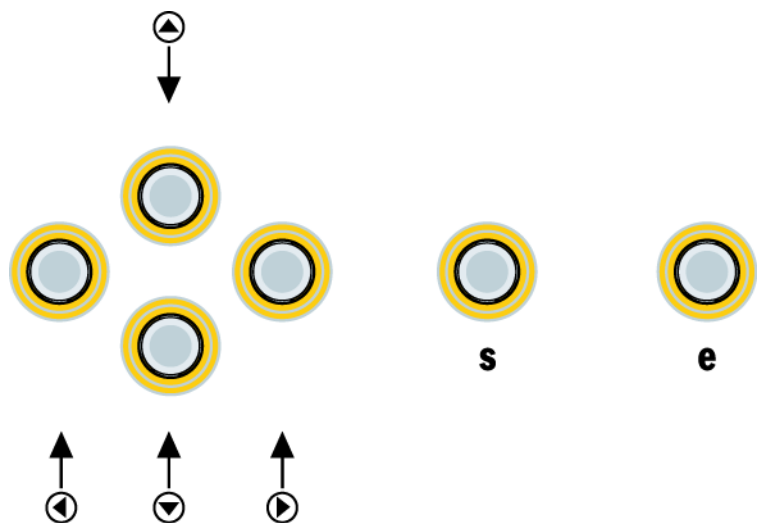


Table 3-2 describes the function of the front panel controls. Use these controls to input your information. The up, down, left, and right buttons do not physically have arrows on the buttons. We use these symbols in text to describe how they work.

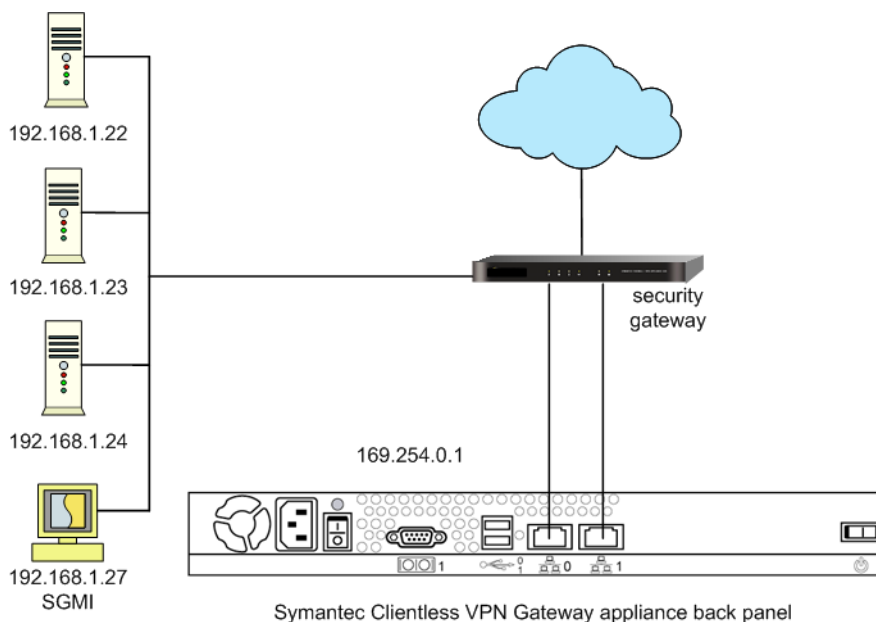
Table 3-2 Front panel controls and how they function

Buttons	Function
Up (>) and down (V) buttons	Increment and decrement the current number displayed on the LCD or to move to the previous menu item (up button) or to the next (down button) menu item.
Left (<) and right (>) buttons	Move across the LCD panel or to move to the previous menu item (left button) or to the next (right button) menu item.
e (Enter)	Launches the System Menu when the appliance is in monitoring mode. Accepts the current value displayed in the LCD when entering information.
s (Select)	Cancels the current action.

Example network diagram

Figure 3-3 provides a sample of a typical network. The Clientless VPN Gateway is managed by a client computer with a browser. Supported browsers include Microsoft Internet Explorer version 6 or later or Netscape version 7 or later. You browse to the specific appliance interface and then type a user name and password to log onto the Security Gateway Management Interface.

Figure 3-3 Example Clientless VPN Gateway appliance typical network



Using the network setup worksheet

During the Clientless VPN Gateway appliance setup process, you enter network address information. Once you enter that information, the appliance's LCD screen displays one password that you need to initiate remote management. This password is used for the administrator password. Use the worksheet to make note of this information.

Make a copy of this form and store the completed form in a secure location. This form serves as a permanent record for each Clientless VPN Gateway appliance installed at your site.

Network setup worksheet

User input during initial setup

To configure an interface for appliance management, you need the following:

Interface IP address _____

Netmask _____

Default Gateway _____

Symantec Clientless VPN Gateway appliance output during initial setup

Record the Administrator password from the LCD display:

Administrator password¹ _____

¹ The password is output during the hardware setup process. This password is also used as the administration password. You can change this password independently from the SGMI or the Command-line interface. This password is used to unlock the front panel controls.

Changing passwords

There are two ways to change a password:

- Use Security Gateway Management Interface > Sever tab > Password.
- Run the appliance setup and accept the new administrator password by selecting [Yes].

For details on changing passwords, see the *Symantec Clientless VPN Gateway 4400 Series Administrator's Guide*.

Performing the initial appliance network setup

This section covers the initial appliance network setup. The Clientless VPN Gateway has two active network interfaces; 0 and 1. Choose an interface to configure for appliance management. Once the interface is setup you can configure the appliance using the Security Gateway Management Interface (SGMI) or the Command-line Interface (CLI) through that interface. See the *Symantec Clientless VPN Gateway 4400 Series Administrator's Guide* for more information.

You must configure the second interface using the SGMI or CLI. See the *Symantec Clientless VPN Gateway 4400 Series Administrator's Guide*.

Configuring the management interface

The following procedure let you configure the management interface of the appliance from the LCD panel on the front of the appliance. After you finish this procedure you can connect to the SGMI or CLI from the configured interface. See [“Connecting to the appliance”](#) on page 28. You use the administrator password generated from this setup procedure to access the appliance from the SGMI and CLI.

Note: To turn off the appliance without beginning setup, press the down arrow on the front panel until you see 3. Shutdown on the LCD screen. Press the e button to confirm shutdown. When you see System Halted on the LCD screen you can turn off the appliance using the power switch on the back panel.

When you turn on the appliance you see the message:

Symantec CVG 5.0

To configure an interface of the appliance

- 1 To start the initial network interface setup on the front panel, press e.

- 2 When the system messages display on the LCD, press any arrow button to display the 1. Network system menu option.
- 3 Press **e** to start the network setup.
- 4 Under Select Interface, use the left or right arrow button to select Interface 0 or Interface 1 for your management interface.
- 5 Press **e**.
- 6 Under Int0 IP Address, enter the inside IP address.
Each octet of the IP address is a separate field in the display. Use the left and right buttons to move between the fields of the IP address. The selected field is surrounded by brackets ([]). Use the up and down buttons to change the number in the field that is selected.
- 7 Press **e**.
- 8 Under Netmask, enter the netmask address for the IP address you just entered.
Each octet of the netmask address is a separate field in the display. Use the left and right buttons to move between the fields of the IP address. The selected field is surrounded by brackets ([]). Use the up and down buttons to change the number in the field that is selected.
- 9 Press **e**.
- 10 Under Default Gateway, enter the default gateway IP address.
Each octet of the netmask address is a separate field in the display. Use the left and right buttons to move between the fields of the IP address. The selected field is surrounded by brackets ([]). Use the up and down buttons to change the number in the field that is selected.
- 11 Press **e**.
- 12 Under Save Setup, use the left or right buttons to select one of the following:

[Yes]	This generates the administrator password. A new password is generated each time you save this setup from the front panel. Use this password to log in to the SGMI or the CLI. You can change the passwords using the SGMI or CLI.
[No]	The configuration is not saved, the system restarts, and all your information is lost. The default selection is [No]. If you select [No], you will exit setup when you press e .
- 13 Press **e**.

The password displays. Record it and store in a secure location. Passwords are case-sensitive.

14 Press **e**.

The following message displays on the LCD:

The Network is now configured.

Caution: Do not repeat this procedure to configure the second interface. Use the SGMI or CLI to configure the second interface.

The LCD screen displays the system menu. After a period of inactivity, the LCD screen then displays the time and status messages.
You can now configure the appliance using the Security Gateway Management Interface (SGMI) or the Command-line Interface (CLI) from the inside interface. See the *Symantec Clientless VPN Gateway 4400 Series Administrator's Guide* for more information.

Displaying system information

Once you complete the initial network appliance setup the LCD screen enters a monitoring mode that it remains in during normal system operations. When in monitoring mode, the appliance LCD displays system information related to the health and status of the appliance. This system updates approximately every second. You can determine the status of your system with the LCD screen. [Table 3-3](#) describes the general LCD screen system fields.

Table 3-3 General system fields description

Field	Description
HH:MM:SS	Displays time of day in hour:hour, minute:minute, second:second format.
Log Disk xx%	Shows the percentage of log partition filled.
Int0 xxxxMb/s	Shows the throughput rate for the inside interface (Mbps).
Int1 xxxxMb/s	Shows the throughput rate for the outside interface (Mbps).
MEM xx%	Shows the percentage of memory usage.
Users xxxxx	Shows the number of connected users.
CPU xx%	Shows the percentage of CPU usage.

Using the system menu

When your appliance is running, you can access the system menu on the appliance by pressing any button on the front panel. You can then select the system menu by pressing the **e** button. By using the arrow buttons, you can view the various system menu options. Press the **e** button to select a menu item. For descriptions of the buttons on the appliance front panel and the functions they perform see “[Front panel controls](#)” on page 20.

[Table 3-4](#) describes the System Menu options.

Table 3-4 System Menu options

System Menu option	Description
1. Network	The system prompts you to enter or change network settings. To continue to the next system menu entry, press either the down button or the right button.
2. Reboot	The system prompts you to select [Yes] or [No]. [No] is selected by default. To reboot, use a button to move the cursor to [Yes] and press e .
3. Shutdown	The system prompts you to confirm system shutdown. Select [Yes] or [No]. Press e again to enter your selection.
4. System ID	Displays the Symantec system ID. Press e to return to the system menu once the Symantec system ID is displayed on the LCD screen. Press either the down button or the right button to move to the next menu item.
5. Factory reset	If you select this menu item, you are prompted to confirm with [Yes] or [No]. Note: If you select [Yes], the appliance returns to its default state and loses any software patches that have been applied. This is the state it was in when you first received the appliance. All network information and configuration data you have entered is lost. Only licensing information, if you entered any, is retained.
6. Diagnostics	Displays the system status information.

About the Security Gateway Management Interface

You access the Security Gateway Management Interface (SGMI) by browsing to the IP address of your appliance from a client computer. You can manage all functions, including secure tunnels and hardware system management, such as

reboots or shutdowns. The same interface is available on all appliances. You can manage many appliances, one-by-one using the SGMI. For a detailed description of the SGMI, see the *Symantec Clientless VPN Gateway Administrator's Guide*.

Connecting to the appliance

After initial setup and reboot, you are ready to configure your appliance. For optimal screen resolution, set your display settings to a minimum of 1024 x 768.

Note: If you are going to manage your Clientless VPN Gateway from a network that is not directly connected to the appliance, you must configure your security gateway to allow HTTPS on port 779.

Before you begin, you need the following information:

- User name (admin) and password you received when you set up the appliance.
- List of all the required IP addresses.
Fill out the worksheets in Appendix A to gather your information.
- If you have your license files, you can upload them on SGMI Server tab License option or you can use the 30-day evaluation (optional). See [“Using the Symantec License Request & Maintenance Web site”](#) on page 74.

To connect to the Clientless VPN Gateway appliance

- 1 Browse to the IP address of the appliance you want to configure. The path is:
https://<IP address of the Symantec Clientless VPN Gateway 4400 Series>:779/
- 2 In the Log on dialog box, do the following:
 - In the user name text box, type admin.
 - In the password text box, type the password you received and wrote down during the appliance LCD setup.
 - Click **Login**.
The SGMI displays.

For a detailed description of the SGMI, see the *Symantec Clientless VPN Gateway Administrator's Guide*.

Configuring your Clientless VPN Gateway appliance

After you have successfully connected to the Clientless VPN Gateway appliance, the system displays the SGMI. For more detailed instructions about how to configure the Clientless VPN Gateway see the Symantec Clientless VPN Gateway 4400 Series Administrator's Guide.

Locking front LCD panel controls

Locking the appliance front LCD panel controls provides additional security against personnel who should not have access privileges. You can lock the front panel controls with the SGMI.

To lock the front LCD panel controls

- 1 On the SGMI, on the Server tab, in the left pane, select Network Access.
- 2 In the right pane under, select Access Methods, next to LCD, check OFF, to lock the front LCD panel controls.

Unlocking the front LCD panel controls

You can unlock the LCD panel and associated navigation buttons with your admin password, but it locks again after 60 seconds of inactivity. To unlock the front LCD panel controls for a longer period of time, you must use the SGMI.

To unlock the front LCD panel controls

- 1 On the SGMI, on the Server tab, in the left pane, select Network Access.
- 2 In the right pane, under Select Access Methods, next to LCD, check ON, to unlock the front LCD panel controls.

Using the command-line interface (CLI)

You can access the Command-line interface (CLI) using any standard terminal program, such as HyperTerminal on Windows or `tip` on Unix, and connecting to the serial console port on the back panel of the appliance. You can also access the CLI from an SSH client.

To setup HyperTerminal to communicate with the CLI

- 1 On your computer, on the connection's Properties Settings tab, on the ASCII setup, clear "echo typed characters locally".
- 2 Make sure your COM1 Properties settings are correct.

See “[Settings for HyperTerminal CLI connection](#)” on page 30.

Table 3-5 Settings for HyperTerminal CLI connection

Parameter	Setting
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None
Hardware handshake	No
Emulation	ANSI

To open a command-line session to the Clientless VPN Gateway appliance

- 1 Connect the null modem serial port cable from your computer to the serial console port on the back of the appliance.
- 2 On your computer, start the HyperTerminal, tip, or SSH client program.
- 3 At the prompt, log on using the default administrator account.
The default username is admin and the password is the one generated during the LCD setup. See “[Performing the initial appliance network setup](#)” on page 24.

```
setup login: admin
password: *****
```

The Clientless VPN Gateway displays the CLI prompt.

See “[Command-Line Interface \(CLI\) features](#)” on page 32.

Running the Quickstart Wizard (Optional)

The Clientless VPN Gateway appliance has a Quickstart Wizard that runs from the CLI. It displays a sequence of questions to help you set up the basic network parameters of the appliance. The Quickstart Wizard allows you to configure the hostname, DNS information, and a quick demonstration environment. Running the Quickstart Wizard is optional. You can configure the Clientless VPN Gateway from the SGMI or CLI. You should only use the Quickstart Wizard if you want to use the demonstration environment. The demonstration environment includes:

- Creating a Demo user (password: Secret)

- Creating an Office role associated with the user
- Creating an access control rule to allow HTTP for demo user

For demonstration environment setup to work properly, the FQDN of the Clientless VPN Gateway must be resolvable by the client system trying to connect. Use HOST files for temporary mappings.

You can change information entered in the Quickstart Wizard or the LCD setup using the SGMI, see the *Symantec Clientless VPN Gateway Administrator's Guide* for more information.

Before starting the Quickstart Wizard, gather the following information:

- Clientless VPN Gateway IP address and mask
- Default gateway IP address
- DNS (Domain Name System) server IP address
- New administration password from the LCD setup
- Clientless VPN Gateway Fully Qualified Domain Name
- Determine if you are using DHCP.

To run the quickstart wizard

- 1 Power on the Clientless VPN Gateway.
- 2 Open a command-line session to the Clientless VPN Gateway appliance.
- 3 Log on using the default administrator account, at the setup login prompt type `admin`
- 4 At the password prompt type your admin password.
The default username is admin and the password is the one generated during the LCD setup. See [“Performing the initial appliance network setup”](#) on page 24.
- 5 Run the Quickstart Wizard, type the following command:
`quickstart`
The Clientless VPN Gateway displays the following prompt:
`Configure your SCVG`
The Quickstart Wizard displays a sequence of questions.
- 6 At the Primary DNS server address prompt, type the IP address of the primary DNS server, for example:
`DNS_IP`
- 7 At the Hostname prompt, type the fully qualified domain name (FQDN) of the Clientless VPN Gateway, for example:
`SCVG_DN`

- 8 To pre-configure the Internal authentication server, at the Use the internal authentication server prompt, type: **yes**
You must type the full word: yes or no. Typing yes starts the Internal authentication server and creates a Role called officeRole, a Scheme (SCVGScheme), and a test user (demo).
- 9 To pre-configure a simple access rule and Quicklink, at the Pre-configure an http-only access rule the default user prompt, type yes,
- 10 At the Hostname to grant HTTP access to (‘*’ for all hosts) prompt type one of the following:
 - A host name to give access to a specific system
 - * (an asterisk) for to give access to all hosts

Hostname to grant HTTP access to (‘*’ for all hosts)

The Clientless VPN Gateway creates a simple rule and assigns the rule to officeRole; this rule allows the demo user (and other members of the officeRole) to access the host through the user interface.
- 11 When the Quickstart Wizard is complete, it displays:
`Quickstart has finished`
- 12 Use the PING command to PING another computer on the LAN from the Clientless VPN Gateway to verify the connection.
- 13 To exit the command-line interface, type the following command: exit.

See [“About the Security Gateway Management Interface”](#) on page 27. To continue configuring the Clientless VPN Gateway appliance for your network, log on to the SGMI.

For a demonstration of the system, sign in to the user interface with the demo account that was automatically configured by the Quickstart Wizard.

Command-Line Interface (CLI) features

For convenience the Command-line interface has the following features:

- Uniform command formats
- Auto-complete
- Auto-list

Uniform command formats

Commands always start with an object followed by the action and then attribute value pairs:

```
object action name1=value1 name2=value2
```

This example shows the definition of network interface 1.

```
ip show interfaceID=1
```

Interface	IP	Netmask
1	172.16.0.1	255.255.255.0

```
Command completed successfully
```

Auto-complete

Auto-complete lets you enter the first few letters and then press tab to auto-complete a command.

Auto-list

If there are multiple possible completions, press tab again to see a list.

Example:

```
i  
interface ip
```

To display a list of all objects, press tab twice without entering data.

Configuring the Ethernet port

You can reconfigure the Clientless VPN Gateway internal Ethernet port (int0) from the command-line interface. The the Clientless VPN Gateway internal Ethernet port (int0) is first configured during the LCD setup. See [“Performing the initial appliance network setup”](#) on page 24.

To configure an Ethernet port

- 1 Open a command-line session on the console from the computer to the Clientless VPN Gateway.

- 2 Log on using the default administrator account, at the setup login prompt type `admin`
- 3 At the password prompt type your admin password.
The default username is admin and the password is the one generated during the LCD setup. See [“Performing the initial appliance network setup”](#) on page 24.

- 4 At the command prompt, type: `ip show`.
This displays the current IP address assigned to the Ethernet port.
`ip show`

Interface	IP	Netmask
0	172.16.0.1	255.255.255.0
1	192.168.0.24	255.255.255.0

Command completed successfully
The number in the Interface column is the interface port number as labeled on the Clientless VPN Gateway.

- 5 Using the IP delete command remove any pre-defined information, type the following command:
`ip delete ip=172.16.0.1`
Command completed successfully
`ip delete ip=192.168.0.24`
Command completed successfully
The IP delete command will disable any remote (SSH) administration sessions.
- 6 To verify that the interface information was deleted, type the following command: `ip show`

Interface	IP	Netmask
-----------	----	---------

Command completed successfully

- 7 To create a new IP definition for the NIC in interface 1, type the following command.
`ip create interfaceID=1 \`
`ip=SCVG_IP netmask=SCVG_Mask`
Command completed successfully

The SCVG_IP and SCVG_mask are the IP address and netmask assigned to your appliance on the internal network. Enter the IP address and netmask in numeric dotted quad format (for example 123.12.1.221).

- 8 To verify the definition, type the following command: `ip show`

Interface	IP	Netmask
1	SCVG_IP	SCVG_Mask

Command completed successfully

Adding the default gateway

This section explains how to add the default gateway from the command-line. You must define a default gateway to access the Web-management interface from a different subnet.

Note: If a computer with a Web browser is connected to the same subnet as the Clientless VPN Gateway, you may complete the configuration using the Security Gateway Management Interface instead of using the command-line interface as shown here. See the *Symantec Clientless VPN Gateway Administrator's Guide* for more information.

Adding the default gateway

- 1 On your console computer, to display the routing rules, type the following command: `route show`

IP	Gateway	Netmask	InterfaceID
SCVG_IP	0.0.0.0	SCVG_Mask	1

Command completed successfully

The InterfaceID number is the Ethernet port number as labelled on the Clientless VPN Gateway.

- 2 To create a default gateway, type the following command:

```
route create ip=0.0.0.0 \  
netmask=0.0.0.0 gateway=Gateway_IP
```

Command completed successfully

The Gateway_IP is the IP address of the default gateway.

- 3 Use the route show command to verify the routing rule, at the prompt type:
route show

IP	Gateway	Netmask	InterfaceID
SCVG_IP	0.0.0.0	SCVG_Mask	1
0.0.0.0	Gateway_IP	0.0.0.0	1

Command completed successfully

- 4 Verify that the network settings are correct by pinging another host that is on the same subnet as the Clientless VPN Gateway appliance, type the following command:

ping another_host_IP

Pinging another_host_IP with 32 bytes of data:

--- another_host_IP ping statistics ---

- 5 Log out to close the session, type the following command:
exit

Restoring the software

The Symantec Clientless VPN Gateway 4400 Series CD-ROM ships with the appliance and contains a Symantec Clientless VPN Gateway 4400 Series restore program. In the unlikely event that a complete reinstallation of the software image on the appliance is required, you can boot this CD-ROM in a computer connected to the appliance.

Note: Before you use this procedure, contact Symantec Technical Support as this operation results in the complete overwriting of your existing appliance configuration. All configuration data is lost. For information on preserving your configuration settings, see the *Symantec Clientless VPN Gateway Administrator's Guide* for backup and restore procedures.

The requirements for the computer running the operating system restore program are as follows:

- An industry-standard computer with a BIOS that lets you start from a IDE CD-ROM.
- An installed 10/100 or 10/100/1000 MB network interface card.
When you receive your restore CD, place it in the computer that you would use in the event you needed to restore your software. Once the CD boots, it will tell you whether or not it found the appropriate hardware to continue

the process. If it cannot use your network card, please locate another computer with a different network interface type.

- Either a crossover cable (supplied) to connect the appliance directly to the int0 network interface on the computer or a connection to a switch or hub to which the appliance is attached.

During the restore process, the appliance will automatically reboot and perform other installation tasks. You must allow this process to complete without interruption for a successful restore of the appliance software to its original factory condition. This process may take 15 minutes.

To restore the appliance operating system

- 1 Press any button on the front panel of the appliance until the System Menu displays on the LCD screen.
- 2 Press the down button until the Shutdown option appears.
- 3 Press **e**.
- 4 When prompted, turn off the power using the power switch.
- 5 Ensure that the PC that you use to restore the system is set to boot from the CD-ROM drive.
- 6 Insert the appliance IDE CD-ROM into the CD-ROM drive.
- 7 When the program runs, you are prompted to accept the Symantec Software License Agreement and directions for the procedure also displays.
- 8 While pressing and holding down the **s** button on the front panel controls, turn on the power to the appliance using the power switch.
- 9 Continue holding down **s** until “Network Boot?” appears in the LCD display.
- 10 Release and press **s** to begin network booting the appliance from the Symantec Clientless VPN Gateway 4400 Series CD-ROM. The LCD display shows the “Network Boot? Loading ...” message.

Other messages you may see consist of the following:

```
Building System
Copying files
Rebooting system
Symantec Diagnostics
Installing software
```

This step may take 15 minutes, and includes the appliance rebooting itself.

- 11 Wait until “Please wait for poweroff” appears on the LCD display. The restore process is now complete.

If your appliance does not turn off after 30 seconds, then turn the unit off manually.

- 12 Remove the CD-ROM and restart your computer to return it to normal service.
- 13 Turn on the appliance and perform the initial setup process again.
See [“Performing the initial appliance network setup”](#) on page 24.

License setup

This chapter includes the following topics:

- [About license files and licensing](#)
- [Getting started with your 30-day grace period](#)
- [Obtaining and organizing license serial numbers](#)
- [Using the Symantec License Request & Maintenance Web site](#)
- [Uploading your license files](#)
- [Explanation of the appliance licensing and maintenance](#)
- [About Symantec Clientless VPN Gateway 4400 Series licenses](#)

About license files and licensing

This chapter covers information about how to obtain a license file. In addition, it covers a general explanation of licensing and maintenance and how it applies to your product.

Getting started with your 30-day grace period

Each appliance requires a license to operate. As a minimum you must purchase a base license with each appliance you purchase. Once you received the license certificate you must activate the license and receive a license file. The license file is loaded onto the appliance to enable applications. To give you time to organize the licensing process, all the software included with your Symantec Clientless VPN Gateway 4400 Series is enabled for a 30-day grace period. Once you load and enable your license file, your 30-day grace period is no longer valid.

Obtaining and organizing license serial numbers

The following five easy steps provide for a successful license implementation:

- Gather your Serial Number Certificates
- Sort your serial numbers for each appliance
- Collect product and contact information
- Plan for your license file
- Obtain your license file

Gather your Serial Number Certificates

The first step in the process is to gather all your Serial Number Certificates. Symantec provides evidence of your purchase by means of a Serial Number Certificate. Check with your sales representative on how your certificates will be sent. Each Serial Number Certificate may contain several unique serial numbers, one for each license or service ordered.

Sort your serial numbers for each appliance

Serial numbers on Serial Number Certificates correspond to a particular order that you have placed, and may not apply to a particular appliance. If you have placed orders for other Symantec products, you may find that the license serial numbers appear intermingled on the same Serial Number Certificate. For example, if you ordered one appliance, you won't have to worry about separating out numbers. If you ordered more than one appliance, your serial numbers will be combined in the Serial Number Certificates and must be separated out.

This document provides a License File Organization Worksheet to ensure that you clearly identify which license serial numbers are used for each appliance prior to generating for your license file. Make a copy of this worksheet for each appliance you ordered, and complete each worksheet prior to obtaining your license file. See [“License File Organization Worksheet”](#) on page 43.

Collect product and contact information

You need the following information when completing the License File Organization Worksheet:

- The appliance serial number.
- The Symantec System ID.
- The email address of the person to whom your license file for this appliance should be sent.
- Names, phone and FAX numbers, and email addresses of two technical contacts.

- Full company name.
- Maintenance serial number for base license.

The Symantec System ID is an ID number that identifies your appliance to the licensing system, which you can find through the product's GUI or command-line interface using the license command.

Warning: The Symantec System ID is case sensitive.

You can locate the appliance serial number on a label on the bottom of your appliance and also on the shipping carton.

Technical contact information (names, phone and FAX numbers) is required as only these two people can contact Symantec for technical support. If you have more than one appliance you may only have two contacts for your entire company.

You must register for maintenance services at the same time that you request your license file.

Complete the License File Organization worksheet recording the serial numbers for the appliance.

The base license includes one year of Gold Maintenance service.

Plan for your license file

When your license file is emailed to you, the only identifying information you receive is in the subject line of the email. The subject line contains one of the serial numbers included inside the license file. You must check your records and verify to which appliance the license email applies and rename the file accordingly. You should create a distinguishable naming convention to easily identify the licenses when you go to upload this license file to the individual appliance.

Your license file is attached to your email in a .zip file. Open this file using a decompression utility, such as WinZip or WinRAR.

The .slf file contained within the .zip file is the actual license file that you must load into your product to make it function.

Do not attempt to edit the .slf file in a text editor such as Notepad or Wordpad as this will corrupt your license file and prevent your product from working properly.

If you need additional support, use the following URL to contact the Customer Service team for your region:

<http://www.symantec.com/licensing/els/help/en/help.html>

You must upload your license file to the appliance before the 30-day grace period expires.

Obtaining your license file

To obtain your license file, browse to <https://licensing.symantec.com> and generate your license.

Organizing your license files

Use the License File Organization Worksheet to organize your license files for each appliance. See “[License File Organization Worksheet](#)” on page 43. Make as many copies of it as you have appliances. When you apply for your license file, ensure that you associate the email, and associated attachment, that you receive from Symantec with a specific appliance. You should create a folder structure to collect and sort the license files you receive with a naming convention that helps you identify which file goes with which appliance.

Your license file email includes a feature serial number in the subject line. You should rename your license file attachment to associate it to the proper appliance. This ensures that the license file has an ID attached to it that you can later track back to the specified appliance.

Note: Once you detached the license file from your email, it is not easy to determine to which appliance it is associated, unless you rename it.

You must fill out the worksheet in [Table 4-1](#) before you apply for your license file.

Table 4-1 License File Organization Worksheet

I. Certificate number			
II. Appliance serial number			
III. Symantec System ID number			
IV. Base Symantec Clientless VPN Gateway license			
Part codes	Description	License sessions	Serial number
	Base license	50	
	Base maintenance		
V. VPN sessions (Additive)			
Part codes	Description	License sessions	Serial number

Using the Symantec License Request & Maintenance Web site

The Symantec Clientless VPN Gateway 4400 Series software is shipped with a license that lets the software operate for 30 days. This license begins when you install the product. You must obtain a license file within the 30-day grace period to continue using the product.

Activating your license files

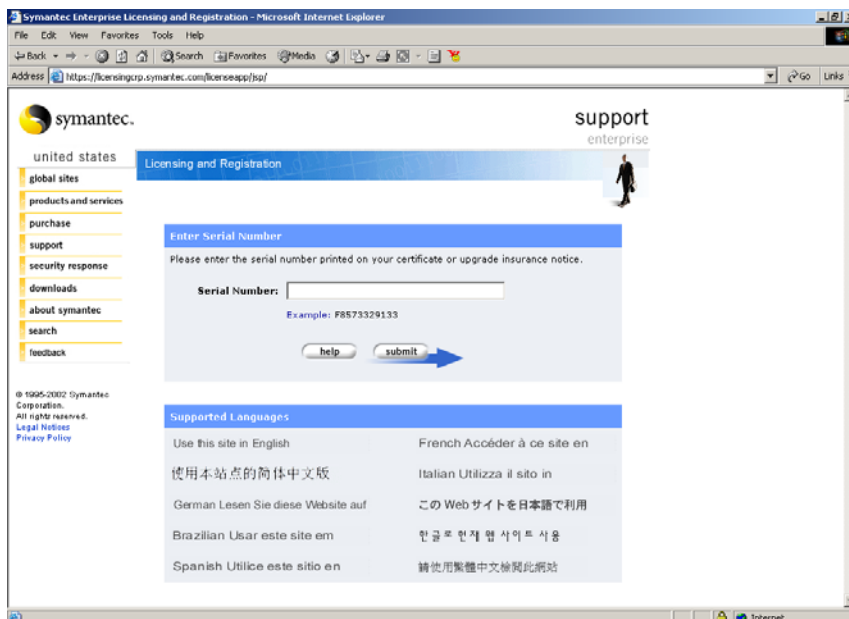
To activate your license you must have the base Software Serial Number Certificate. This is the first level of information you are prompted for from the licensing Web site.

Note: The license file you generate applies to one appliance only.

If you are increasing the number of sessions for this appliance, have those serial numbers ready as well. When you apply for your license file, be aware that all the serial numbers you input apply to a specific appliance. Do not mix serial numbers that apply to other appliances.

To activate your license files

- 1 Browse to <https://licensing.symantec.com>.



- 2 Under Supported Languages, select your language.
- 3 In the Licensing and Registration page, under Enter Serial Number, in the Serial Number text box, type your base software serial number.
This is the serial number found on the base Software Serial Number Certificate for the base license.

4 Click **submit**.

symantec support enterprise

united states
global sites
products and services
purchase
support
security response
downloads
about symantec
search
feedback

© 1995-2003 Symantec Corporation. All rights reserved. [Legal Notices](#) [Privacy Policy](#)

Licensing and Registration

Enter Your Email Address, Symantec System ID, and any additional Serial Numbers

- Enter a valid email address. Your license file will be sent to this address.
- A valid Symantec System ID is required to activate the product on a specific machine. Your product documentation contains instructions for obtaining your Symantec System ID.
- Enter any additional serial number you wish to register on the same machine for the same product. Click on the 'add' button to add more serial numbers.

Email Address :
Example : name@myaddress.com

Symantec System ID :
Example : (1:000476d87a27)

Serial Number 1:

Serial Number 2:

Serial Number 3:

[help](#) [add](#) [submit](#)

- 5 Under Enter Your Email Address, Symantec System ID, and any additional Serial Numbers, do the following:
- In the Email Address text box, type the email address of the person managing the license files.
The license file is mailed to this address.
 - In the Symantec System ID text box, type your appliance Symantec System ID.
A valid Symantec System ID is required to activate the product on a specific machine. You can find the Symantec System ID using the Symantec Gateway Management Interface on the Server tab, on the left pane License menu option, under Obtain New Licenses For The Symantec Clientless VPN Gateway.

Warning: The Symantec System ID requires the parenthesis and must look like (4:E978A321). Do not omit the parenthesis.

- In the Serial Number text boxes, type any additional appliance serial numbers, which you can find on the Serial Number Certificates. Include your maintenance serial number for this appliance. It does not matter which order the numbers are typed.

These are serial numbers that are associated with licenses purchased for this appliance only.

- 6 If you have more than three serial numbers to enter, click **add**.
Clicking add inserts new fields above the ones you have already filled in. You can now input any additional serial numbers you may have. You can click add as many times as you need to add all of your serial numbers.
- 7 When you are finished, click **submit**.
- 8 Under Please enter your Appliance Serial Number, in the Appliance Serial Number text box, type the appliance serial number.
You can find the appliance serial number on the label on the bottom of the appliance.

symantec. support enterprise

united states

Licensing and Registration

global sites

products and services

purchase

support

security response

downloads

about symantec

search

feedback

Please enter your Appliance Serial Number

Please enter your Appliance Serial Number

Appliance Serial Number:

Example: FLX1234567890

submit

© 1995-2003 Symantec Corporation.
All rights reserved.
[Legal Notices](#)
[Privacy Policy](#)

9 Press **submit**.

symantec. support enterprise

united states
global sites
products and services
purchase
support
security response
downloads
about symantec
search
feedback

© 1995–2003 Symantec Corporation.
All rights reserved.
[Legal Notices](#)
[Privacy Policy](#)

Licensing and Registration

Please enter your technical contact information.
Please enter your technical contact information.
Please enter all of the requested information using latin characters only.
Bold fields are required.:

Contact 1

First Name :
Middle Name:
Last Name:
Work Phone:
Mobile Phone:
Pager:
Email Address:

Contact 2

First Name :
Middle Name:
Last Name :
Work Phone:
Mobile Phone:
Pager:
Email Address:

submit

10 On the technical contact information page, under Contact 1, do the following:

- In the First Name text box, type the first name of your technical contact.
- In the Last Name text box, type the last name of your technical contact.
- In the Work Phone text box, type the phone number of your technical contact.
- In the Email Address text box, type the email address of the technical contact.

If you have an additional contact, fill in the information under Contact 2.

11 Click **submit**.

symantec. support enterprise

united states Licensing and Registration

global sites
products and services
purchase
support
security response
downloads
about symantec
search
feedback

© 1995-2003 Symantec Corporation. All rights reserved. Legal Notices Privacy Policy

Confirm the following information

Please confirm the following information. If required, click on the corresponding "modify" button to correct an item.

Serial Numbers

Serial Number	Product	modify
L1872893345	Symantec Clientless VPN Gateway 5.0 - Base 50 Session License	←

License Registration

Email Address: jdoe@acme.com ← modify

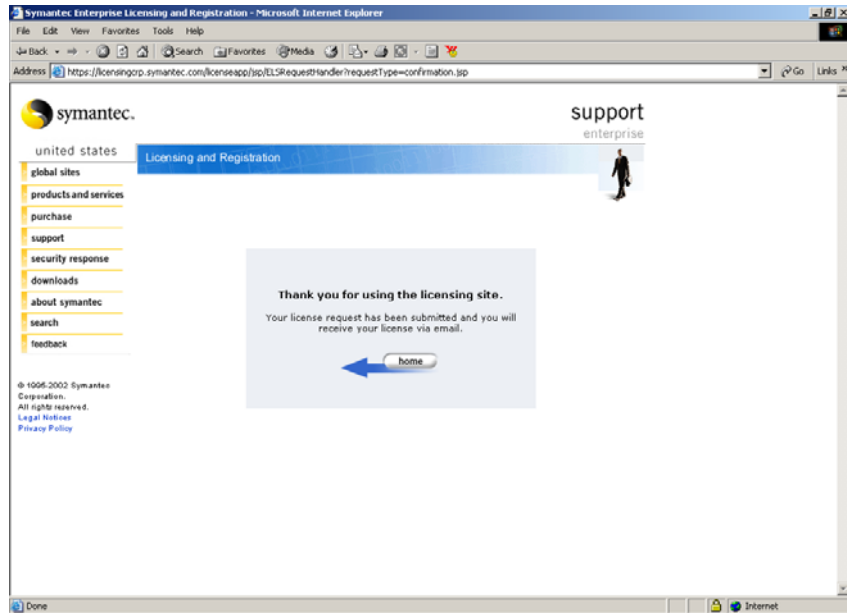
Symantec System ID: (4:E978A321)

help submit →

12 Under Confirm the following information, do the following:

- Under Serial Numbers, confirm the serial numbers and products you have registered.
- Under License Registration, confirm your email address and Symantec System ID.
- Under Support Registration, confirm your maintenance serial number, and the two support contacts for your product.
- Under Appliance Registration, confirm your hardware serial number, name, company name, company address, work phone, and email address for a company contact responsible for this product.

13 Click **submit**.



The person you specified receives an email from Symantec with an attached license file, which he or she can use to enable all the product features registered. The subject line of that email contains a serial number for one of the licensed products contained within the order. Copy your license files to a known directory, rename them, and move them to a system you use to manage your appliance.

Note: Once you receive, rename, and store your license files, keep a back-up of these files in a safe place.

If you purchase additional licenses for this appliance in the future, you should follow these same steps for the new licenses and associated serial numbers. Note that old serial numbers are not reentered. Multiple license files are applied to a single appliance and licenses are additive.

Uploading your license files

If you have already completed your initial setup and configuration, have been using your 30-day grace period, and are now ready to install your license files, you can install your licenses by going to the Symantec Gateway Management

Interface > Server tab > Licenses window, or use the CLI and the license command.

To upload your license files

- 1 In the Symantec Gateway Management Interface, on the Server tab, in the left pane, click **License**.
- 2 In the right pane, under Obtain New Licenses For The Symantec Clientless VPN Gateway, click **Browse**, and browse to where you have saved your license files, and select a license file.
- 3 Once you have located your license file, click **Upload**.

Removing license files

If you must remove a license file, contact Symantec Technical Support.

Explanation of the appliance licensing and maintenance

Symantec Clientless VPN Gateway 4400 Series usage is controlled by a licensing scheme.

Obtaining a license file

When you purchase a license, Symantec provides you with a software Serial Number Certificate. See [“Obtaining and organizing license serial numbers”](#) on page 40.

Basic license types

Each appliance needs a base license, which includes 50 concurrent sessions. Additive licenses are available to increase the number of concurrent sessions in 25, 100, 250, and 1000 session increments.

License certificates

You must order the appliance with a base appliance license. Symantec sends you the Serial Number Certificate that contains a software serial number, which, when combined with the appliance Symantec System ID, is used to generate a license file.

30-day grace period

The appliance runs for 30 days without a license file. However, a license file is necessary to enable the software on the appliance to run after this 30-day grace period has expired. You obtain a license file by accessing the Symantec licensing Web site. See [“Getting started with your 30-day grace period”](#) on page 39.

Maintenance contracts

Except for the first year, separate one and two year maintenance renewal contracts are available for appliance base license functionality and additive licenses.

Appliance

All base licenses include a Gold Maintenance contract. This Gold Maintenance contract starts from the day the base license is purchased and lasts for one year. The Gold Maintenance contracts include:

- Business-hour telephone support.
- Upgrade insurance, which includes an entitlement to any new versions of the appliance software released by Symantec during the term of the contract.
- Advanced replacement of failed hardware.
If the appliance hardware fails during the term of the contract and this failure is confirmed by Symantec, Symantec ships (during normal business hours) a replacement unit within 24-hours of this confirmation. Symantec has depots around the world to ensure timely delivery of the replacement.

Additive session licenses include maintenance for the increased number of sessions if the base appliance is currently covered by a maintenance agreement. This maintenance is tied to the basic appliance contract and expires on the same date.

Platinum support is available as an uplift to Gold maintenance. The contract co-terminates with the base appliance contract. You must purchase Gold and Platinum renewals at the same time and for the same duration as the appliance renewal.

Maintenance renewals

One and two-year maintenance renewal contracts are available.

Platinum support uplift

You may need continuous availability of telephone support (24 x 7). This is provided for by a Platinum support uplifts to the Gold contract. For subsequent years, Platinum support uplift renewal contracts are also available.

High availability license bundles

High availability license bundles are available to build a cluster of one active machine and one hot standby machine. The hot standby machine's license has been significantly discounted under the condition that the two licenses included in the bundle may not be separated and run on two machines that are not part of a high availability cluster. If you separate these two licenses, you are in violation of your license.

Load balancing license bundles

Load balancing bundles are available to build a cluster of machines which can support more concurrent sessions than a single machine. The licenses for each machine have been significantly discounted under the condition that the licenses may not be separated and run on machines which are not connected to the same hardware load balancer and sharing the same load. If you separate these two or three licenses, you are in violation of your license.

About Symantec Clientless VPN Gateway 4400 Series licenses

The appliance software is covered by the Symantec Gateway Security License and Warranty Agreement. The license agreement grants the licensee the right to use the software on the associated appliance. The LINUX operating system used in Symantec Clientless VPN Gateway 4400 Series is covered by the GNU General Public License (GPL) and the Library General Public License (LGPL). See "[Legal agreements](#)" on page 71.

Developing a pre-installation security plan

This chapter includes the following topics:

- [About developing a security plan](#)
- [Defining your security policy](#)
- [Educating users](#)
- [Filling out worksheets](#)

About developing a security plan

Developing a security plan is your first step in your installation process and helps you collect the information needed to install and configure your Symantec Security Gateway appliance.

The process of developing a security plan consists of three basic steps:

- Defining your security policy
- Educating your users
- Filling out worksheets

Defining your security policy

Before configuring your security gateway, you must understand exactly what network resources and services you want to . It is crucial to have a carefully designed network security policy to guard the valuable resources and information of your organization.

Ideally, your security policy should be captured in a document that describes your organization's VPN needs and concerns. Creating this document is the first step in building an effective overall system and should be done prior to installation.

Your security plan details the implementation of your security policy. Based on the security concerns and trade-offs of your overall policy, your security plan should contain a set of tasks. One of these tasks consists of establishing procedures and rules for access to resources located on your network. These resources include:

- Host computers and servers
- Workstations
- Connection devices (gateways, routers, bridges, and repeaters)
- Terminal servers and remote access servers
- Networking and applications software
- Information in files and databases

Before writing your security plan

Before you begin writing rules to implement your plan using the *Symantec Clientless VPN Gateway Administrator's Guide*, you need to answer the following questions:

- What is your network topology and deployment scenario?
- What types of services, such as Web, FTP, and so on, do you want to allow for internal users?
- To what hosts, subnets, and users do you want to allow these services?
- What external users will have access to your network? Where will they come from and where do you want to allow them to go? During what hours? For what period of time?
- Do you intend to implement a service network?
- What types of services do you want to allow for external users and hosts?
- What type of authentication will you require for external users? (Strong authentication is recommended for any access from public networks.)

Becoming security-conscious

Developing and implementing a security plan for the security gateway you are installing should be only one part of your overall security policy. The security gateway offers the best protection against uninvited entry into your network. However, the Symantec Clientless VPN Gateway 4400 Series cannot guard against entry by people who obtain valid authentication credentials, any more than a sophisticated lock can stop a thief in possession of the right key.

Formulate goals

Take the time to formulate the specific goals of your security plan. Identify the resources you are protecting and all possible threats. Protecting your resources from unauthorized external users maybe only one of your goals. You may also need to limit internal access to certain systems to specific users and groups, within specific time periods. You will need to define these users and groups for the firewall and how to configure special services to be passed through these systems. The *Symantec Clientless VPN Gateway Administrator's Guide* explains how to define users and user groups.

Review issues

You should review your organization's specific issues in detail before you begin configuring the server. Your network's security depends on planning sound

policies, implementing them carefully, and confirming that they work as intended.

Educating users

Your overall site policy involves a numbers of tasks. Of these, user education is paramount. Publish your company's security policy. Make sure your users are informed of the determination of would-be invaders and the sophistication of available password guessing programs. Make sure they understand how common security breaches are and how costly they can be. These facts alone dictate that users should be encouraged to select passwords that are difficult to crack and to change passwords regularly.

Involving the user community

When developing the details of your security plan, you should solicit the input of group managers or leaders on what services they require, for what users, and so on. Explain to users the need for network security to protect private information, intellectual property, and your business plans.

Notifying affected users

Before implementing policies, notify the user community of your proposed policies. Doing so in advance can prevent unnecessary frustration on the part of your users.

For instance, if you plan to limit Web services to a single server during specific hours, let this be known to the affected groups and users. If you plan to pass all email through a dedicated server, or if external users will be disallowed from accessing certain systems by Telnet, consider passing these changes along before implementation. Consulting users prior to implementation may save you the time needed to fine-tune those policies later.

Taking a pro-active stance

Again, keep in mind that configuring a set of authorization rules on the security gateway is just one piece of your overall security plan. To be effective, this plan should also include:

- Physical security of key systems (especially the security gateway)
- Security risk training for users
- Guidelines on passwords
- Proprietary information policies

■ Network planning

Filling out worksheets

To aid you in the planning process, we have provided a set of policy planning worksheets. Use these worksheets to help implement the specific tasks of your security plan and to assist you during the installation process.

Defining your organization

Begin by defining your organization. Here is where you explore your existing security policy, if any; notate who will be assigned as administrators; types of authentication; and how your administrators will be contacted.

To define your existing organization

- 1 Does your organization have a security policy?

_____ Yes _____ No

If you checked No, refer to the first part of this chapter for information relating to the development of a security policy.

- 2 Do you plan to establish special groups or users with different levels of access or control that other groups and users will not have?

_____ Yes _____ No

- 3 Do you plan to establish subnets, users by subnet, or users by authentication?

_____ Yes _____ No

- 4 What are your network access points?

- 5 Name of the primary administrator:

6 Use [Table A-1](#) to list all persons involved in administering the system.

Table A-1 Administrator names

Name	Email	Phone	Pager

7 Are organization computer resources accessible by remote dial-in?

☐ Yes ☐ No

8 Are organization computer resources accessible by an internal network?

☐ Yes ☐ No

9 What communications servers are used? (such as SMTP, Microsoft Exchange)

10 What form of authentication will be used for remote access to company resources?

- ☐ User name/password
- ☐ LDAP
- ☐ Passgo Defender
- ☐ RADIUS
- ☐ Entrust
- ☐ Bellcore S/Key
- ☐ TACACs+
- ☐ RSA SecurID
- ☐ Windows based
- ☐ Other

11 Do you have other security gateways on your network now?

☐ Yes ☐ No

12 If Yes, what brand? _____

13 Do you have third-party firewalls on your network now?

_____ Yes

_____ No

14 If Yes, which one and version? _____

15 Have you created a network diagram? If so, please print and attach.

_____ Yes

_____ No

Site hardware information

Before you begin the installation process, you must collect some basic hardware information.

To collect hardware information for your site

1 Record the Host ID of the Symantec Clientless VPN Gateway 4400 Series.

2 Record the Symantec System ID for the appliance. This is used for licensing. See [“Using the Symantec License Request & Maintenance Web site”](#) on page 74.

The System ID is a decorated Host ID.

Before installation, ensure the host network connections are configured and tested properly. Verify that you can ping the network interfaces of the server from clients on the same network.

3 Record the number of host computers of each type that compose your network.

_____ UNIX

_____ Windows

_____ Other (type) _____

4 What kind of Internet access do you have? What speed?

- 5 Record the name of your Internet Service Provider (ISP).

- 6 Does your site have, or plan to have, more than one Internet access point?

_____ Yes

_____ No

- 7 Are there any other Internet connections besides the security gateway (such as modems connected to workstations)? If yes, list.

_____ Yes

_____ No

TCP/IP address

It is important to think about the TCP/IP requirements for your site. This includes information about running Domain Name Services (DNS), types and names of domains on your network, and making a list of protocols used that need to pass through your security gateway.

To collect TCP/IP address information

- 1 Do you currently run Domain Name Services (DNS) on your network?

_____ Yes

_____ No

- 2 What type of domain structure is in use at your site?

_____ Single domain

_____ Multiple domains

_____ Subdomains

- 3 What type of name service do you provide?

_____ Primary name services

_____ Secondary name services

_____ Internal/private

4 Do you have an internal name server?

_____ Yes _____ No

5 Do you have someone at your site who is knowledgeable about, and comfortable working with, DNS and how to configure it properly?

_____ Yes _____ No

6 If yes, who?

7 Check the address types being used at your site:

_____ Registered IP address _____ Private IP address (RFC 1918)
_____ Unregistered IP address

Your connection to the Internet must have at least one public network address. You should use private, RFC 1918-compliant addresses internally or publicly registered IP addresses.

8 List the address ranges you currently use in your network:

9 List the protocols you use in your network:

10 Will you be using network news services (NNTP)?

_____ Yes _____ No

11 If yes, and you have your own internal NNTP server, record its IP address and the address of the server that will be supplying you with news feeds.

_____ Internal server: _____

_____ External news server: _____

Note: Only IP can be directly handled by the security gateway. Other protocols such as IPX cannot be serviced or passed through the security gateway.

Allowed TCP/IP services

Use the following tables to define all the allowed TCP/IP services in your network.

To define allowed TCP/IP services

1 Use [Table A-2](#) and check the access type (if any) you will allow for the following services:

Table A-2 Allowed TCP/IP access type

Access group	Telnet	SMTP	HTTPS	CIFS	HTTP	NNTP	RealAudio	RTSP	PING	Other
All users										
All internal users										
Selected group										
No access										

2 Use [Table A-3](#) to list your TCP/IP services:

Table A-3 TCP/IP services

	Group	Authentication	Access times
FTP			

Table A-3 TCP/IP services (Continued)

	Group	Authentication	Access times
Telnet			
HTTP			
Other			

Note: Over time, you will likely refine these permissions. You should make periodic updates to this list.

Web service information

Use the following section to define information about your Web services.

To define your Web services

1 Will you be using a Web server?

Yes

No

- _____ External to the security gateway

- Name: _____ Address: _____

- Proxy server name:_____ Address:_____

- _____ Yes _____ No

-

- Table A-4** Special services names

[illegible]

Access lists

List those users and groups to which you plan to write rules to allow access.

Use [Table A-5](#) to list all entity identifications allowed.

Table A-5 Entity identification

[illegible]

Use [Table A-6](#) to list all user identities allowed.

Table A-6 User identification

[illegible]

Defining your network architecture

In the following section, list all of the entities that comprise your network. Show all routers and computers systems that will be directly affected by, or connected to, the security gateway and its directly connected networks. Label each network component with its IP address and network mask.

Use [Table A-7](#) to create a list of all internal servers. Your internal network consists of at least the security gateway host and a router.

Table A-7 Internal network servers

	DNS name services	Mail server	Web server	Other server
Service				
Host name				
IP address				
Subnet mask				

Use [Table A-8](#) to list your security gateway host system addresses.

Table A-8 Security gateway host internal and external IP addresses

Series host	Internal/external IP addresses

Use [Table A-9](#) to list your router IP addresses.

Table A-9 Router IP addresses

Router	IP addresses

Table A-9 Router IP addresses

Router	IP addresses

Your external network can also include external servers, such as an external Web server. Use [Table A-10](#) to list all external network servers.

Table A-10 External network servers

	DNS name services	Mail server	Web server	Other server
Service				
Host name				
IP address				
Subnet mask				

Legal agreements

This chapter includes the following topics:

- [About the Symantec Clientless VPN Gateway 4400 Series licenses](#)
- [SYMANTEC CLIENTLESS VPN GATEWAY APPLIANCE LICENSE AND WARRANTY AGREEMENT](#)
- [Third-party attributions](#)
- [GNU library general public license](#)

About the Symantec Clientless VPN Gateway 4400 Series licenses

The appliance software is covered by the Symantec Clientless VPN Gateway 4400 Series License and Warranty Agreement. The license agreement grants the licensee the right to use the software on the associated appliance. The LINUX operating system used in Symantec Clientless VPN Gateway 4400 Series is covered by the GNU General Public License (GPL) and the Library General Public License (LGPL).

SYMANTEC CLIENTLESS VPN GATEWAY APPLIANCE LICENSE AND WARRANTY AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE INCLUDED WITH THE APPLIANCE YOU HAVE PURCHASED TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") AND TO PROVIDE WARRANTIES ON THE APPLIANCE ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE

TERMS OF THIS LICENSE AND WARRANTY AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AND WARRANTY AGREEMENT CAREFULLY BEFORE USING THE APPLIANCE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, REQUESTING A LICENSE KEY OR USING THE SOFTWARE AND THE APPLIANCE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON IF APPLICABLE AND DO NOT USE THE SOFTWARE AND THE APPLIANCE.

1. Software License:

Except for the software, if any, described in the Excluded Software section at the end of this agreement (the "Excluded Software"), the software (the "Software") which accompanies the appliance You have purchased (the "Appliance") is the property of Symantec or its licensors and is protected by copyright law. Except for the Excluded Software, You agree and acknowledge that You must purchase a separate license for each Software functionality which You intend to use in connection with the Appliance, and activate such Software functionalities as designated by Symantec, prior to using the Appliance. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You as well as the copy of the Software provided to You on a CD-ROM or other media in connection with the Appliance (the "Restore Software"). Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Appliance and/or the Software, Your rights and obligations with respect to the use of this Software are as follows:

You may:

- A. use the Software solely as part of the Appliance for no more than the number of concurrent users as have been licensed to You by Symantec under a License Module;
- B. use the Restore Software solely to restore the Appliance to its original factory functionality in the event the Software preloaded on the Appliance is corrupted or becomes unusable;
- C. make copies of the printed documentation which accompanies the Appliance as necessary to support Your authorized use of the Appliance; and

D. after written notice to Symantec and in connection with a transfer of the Appliance, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software, Symantec consents to the transfer and the transferee agrees in writing to the terms and conditions of this agreement.

You may not:

A. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

B. use the Restore Software for any purpose other than to restore the Appliance to the original factory functionality;

C. use, if You received the Software distributed on an Appliance containing multiple Symantec products, any Symantec software on the Appliance for which You have not received a permission in a License Module; or

D. use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (e.g., antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for each Software functionality which You have purchased and activated for use with the Appliance for any period for which You have (i) purchased a subscription for Content Updates for such Software functionality; (ii) entered into a support agreement that includes Content Updates for such Software functionality; or (iii) otherwise separately acquired the right to obtain Content Updates for such Software functionality. This license does not otherwise permit You to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Restore Software is distributed will be free from defects for a period of thirty (30) days from the date of original purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Restore Software.

Symantec warrants that the Software will perform on the Appliance in substantial compliance with the written documentation accompanying the

Appliance for a period of thirty (30) days from the date of original purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Software returned to Symantec within the warranty period or refund the money You paid for the Appliance.

Symantec warrants that the hardware component of the Appliance (the "Hardware") shall be free from defects in material and workmanship under normal use and service and substantially conform to the written documentation accompanying the Appliance for a period of three hundred sixty-five (365) days from the date of original purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Hardware returned to Symantec within the warranty period or refund the money You paid for the Appliance.

The warranties contained in this agreement will not apply to any Software or Hardware which:

A.has been altered, supplemented, upgraded or modified in any way; or

B.has been repaired except by Symantec or its designee.

Additionally, the warranties contained in this agreement do not apply to repair or replacement caused or necessitated by: (i) events occurring after risk of loss passes to You such as loss or damage during shipment; (ii) acts of God including without limitation natural acts such as fire, flood, wind earthquake, lightning or similar disaster; (iii) improper use, environment, installation or electrical supply, improper maintenance, or any other misuse, abuse or mishandling; (iv) governmental actions or inactions; (v) strikes or work stoppages; (vi) Your failure to follow applicable use or operations instructions or manuals; (vii) Your failure to implement, or to allow Symantec or its designee to implement, any corrections or modifications to the Appliance made available to You by Symantec; or (viii) such other events outside Symantec's reasonable control.

Upon discovery of any failure of the Hardware, or component thereof, to conform to the applicable warranty during the applicable warranty period, You are required to contact us within ten (10) days after such failure and seek a return material authorization ("RMA") number. Symantec will promptly issue the requested RMA as long as we determine that You meet the conditions for warranty service. The allegedly defective Appliance, or component thereof, shall be returned to Symantec, securely and properly packaged, freight and insurance prepaid, with the RMA number prominently displayed on the exterior of the shipment packaging and with the Appliance. Symantec will have no obligation to accept any Appliance which is returned without an RMA number.

Upon completion of repair or if Symantec decides, in accordance with the warranty, to replace a defective Appliance, Symantec will return such repaired

or replacement Appliance to You, freight and insurance prepaid. In the event that Symantec, in its sole discretion, determines that it is unable to replace or repair the Hardware, Symantec will refund to You the F.O.B. price paid by You for the defective Appliance. Defective Appliances returned to Symantec will become the property of Symantec.

Symantec does not warrant that the Appliance will meet Your requirements or that operation of the Appliance will be uninterrupted or that the Appliance will be error-free.

In order to exercise any of the warranty rights contained in this Agreement, You must have available an original sales receipt or bill of sale demonstrating proof of purchase with Your warranty claim.

THE ABOVE WARRANTIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE APPLIANCE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software or the Appliance.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting

of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

6. Export Regulation:

You agree to comply strictly with all applicable export control laws, including the US Export Administration Act and its associated regulations and acknowledge Your responsibility to obtain licenses as required to export, re-export or import the Appliance. Export or re-export of the Appliance to Cuba, North Korea, Iran, Iraq, Libya, Syria or Sudan is prohibited.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Appliance and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software and shall return the Appliance to Symantec. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

8. Excluded Software:

The Excluded Software included with the Appliance consists of General Public License software, including without limitation, Linux distribution and other programs licensed under such Linux distribution, Stunnel, SquirrelMail, pam_ldap 1.6.4, smarty templates 2.5.0, vrrpd 0.6, logrotate 3.6, isolinux 1.75, pam_radius 1.3.15, eepro100-diag c 2.1.1 and Perl 5.6.1. All Excluded Software is licensed under the GNU General Public License, Version 2, June 1991, as published by the Free Software Foundation, a copy of which is included with the user documentation for the Appliance. The license entitles You to receive a copy of the source code for the Excluded Software, including any modifications thereto, only upon request at a nominal charge. If You are interested in obtaining a copy of such source code, please contact Symantec Customer Service at one of the above addresses for further information.

Third-party attributions

A. Apache Software License, v 1.1

"This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)."

B. Mod_SSL Package License

"This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>)."

C. OpenSSL Library License

1. "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

D. SSLeay License

"This product includes cryptographic software written by Eric Young (ey@cryptsoft.com)"

E. The PHP license version 3.0

"This product includes PHP, freely available from <<http://www.php.net/>>".

F. Q Public License, Version 1.0

Copyright (C) 1999 Trolltech AS, Norway.

G. Berkeley DB Software Copyrights, Conditions, and Disclaimers

Copyright (c) 1990-2000 Sleepycat Software. All rights reserved.

Copyright (c) 1990, 1993, 1994, 1995 The Regents of the University of California. All rights reserved.

Copyright (c) 1995, 1996 The President and Fellows of Harvard University. All rights reserved.

H. Libpng Library Requirements, Copyright, and Disclaimer

Linux Loader Requirements, Copyright, and Disclaimer

Linux LOader (LILO) program code, documentation, and auxiliary programs are Copyright 1992-1998 Werner Almesberger. Copyright 1999-2001 John Coffman. All rights reserved.

I. Linux Loader Requirements, Copyright, and Disclaimer

"Linux LOader (LILO) program code, documentation, and auxiliary programs are Copyright 1992-1998 Werner Almesberger. Copyright 1999-2001 John Coffman. All rights reserved."

J. OpenLDAP Public License Version 2.7

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina. All rights reserved.

K. SSH Implementation Requirements, Copyrights, and Disclaimers

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.

Copyright (c) 1983, 1990, 1992, 1993, 1995 The Regents of the University of California. All rights reserved.

Copyright (c) 1995 Patrick Powell

L. Zlib Requirements, Copyright, and Disclaimer

(C) 1995-2002 Jean-loup Gailly and Mark Adler.

M. Popt Requirements, Copyright, and Disclaimer

Software: Copyright (c) 1998 Red Hat Software.

N. Pam Requirements, Copyright, and Disclaimer

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

O. Inetd Requirements, Copyright, and Disclaimer

"Copyright (c) 1990, 1993 The Regents of the University of California. All rights reserved."

P. Ncurses Requirements, Copyright, and Disclaimer

"Copyright (c) 1998,1999,2000 Free Software Foundation, Inc."

Q. Graphviz License Agreement Version 1.2D

"This product contains certain software code or other information ("AT&T Software") proprietary to AT&T Corp. ("AT&T"). The AT&T Software is provided to you "AS IS". YOU ASSUME TOTAL RESPONSIBILITY AND RISK FOR USE OF THE AT&T SOFTWARE. AT&T DOES NOT MAKE, AND EXPRESSLY DISCLAIMS, ANY EXPRESS OR IMPLIED WARRANTIES OF ANY KIND WHATSOEVER, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WARRANTIES OF TITLE OR NON-INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS, ANY WARRANTIES ARISING BY USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE, OR ANY WARRANTY THAT THE AT&T SOFTWARE IS "ERROR FREE" OR WILL MEET YOUR REQUIREMENTS.

R. VRRPD License Terms

(c) JME SOFT

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

Cisco's Policy with respect to VRRP is available at (<http://mail-index.netbsd.org/tech-net/2003/11/24/0000.html>).

S. GNU Free Documentation License Version 1.2 Copyright (C) 2000,2001,2002 Free Software Foundation, Inc.

GNU library general public license

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better. However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a “work based on the library” and a “work that uses the library”. The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

GNU LIBRARY GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called “this License”). Each licensee is addressed as “you”.

A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The “Library”, below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification”.)

“Source code” for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library’s complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a. The modified work must itself be a software library.
- b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the

terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”. The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a “work that uses the Library” uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a “work that uses the Library” with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer’s own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the “work that uses the Library” must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

13. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

16. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE

ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Troubleshooting

This chapter includes the following topics:

- [About troubleshooting](#)
- [Accessing troubleshooting information](#)

About troubleshooting

You can find up-to-date troubleshooting information for Symantec Clientless VPN Gateway 4400 Series (and all Symantec products) on the Symantec Web site, www.symantec.com.

Accessing troubleshooting information

Use the following procedure to access troubleshooting information from the Symantec Knowledge Base.

To access Symantec Clientless VPN Gateway 4400 Series troubleshooting information

- 1 Go to www.symantec.com.
- 2 On the top of the home page, click **support**.
- 3 Under Product Support > enterprise, click **Continue**.
- 4 On the Support enterprise page, under Technical Support, click **knowledge base**.
- 5 Under select a knowledge base, scroll down and click **Symantec Clientless VPN Gateway 4400 Series**.
- 6 Click on your specific product name and version.
- 7 On the knowledge base page for Symantec Clientless VPN Gateway 4400 Series, do any of the following:
 - On the Hot Topics tab, click any of the items in the list to view a detailed list of knowledge base articles on that topic.
 - On the Search tab, in the text box, type a string containing your question. Use the drop-down list to determine how the search is performed and click **Search**.
 - On the Browse tab, expand a heading to see knowledge base articles related to that topic.

Specifications and safety

This chapter includes the following topics:

- [About this appendix](#)
- [Product specifications](#)
- [Safeguard instructions](#)
- [Product certifications](#)

About this appendix

This appendix lists the product specifications and safety certifications.

Product specifications

Each respective model offers increased performance and these different specifications are listed in [Table D-1](#).

Table D-1 Product specifications

Parameter	Model 4420	4460
Length	43.2 cm (17 in.)	61 cm (24.00 in.)
Width	43.2 cm (17 in.)	43.2 cm (17 in.)
Height	4.45 cm (1.75 in.)	8.9 cm (3.50 in.)
Weight	6.17 kg (13.6 lb)	10.3 kg (22.7 lb)
Network interfaces	6 10/100	8 10/100/1000
User interface	2 line x 16 character LCD	2 line x 16 character LCD
Operating temperature range	41° to 91° F (5° to 35° C)	32° to 104° F (0° to 40° C)
Storage temperature range	32° to 104° F (0° to 40° C)	32° to 104° F (0° to 40° C)
Operating humidity	10-80% non-condensing	10-80% non-condensing
Non-operating humidity	95% non-condensing	95% non-condensing
AC power	90-264 VAC	90-264 VAC
Input frequency	47-63 Hz	47-63 Hz
Maximum power capability	300 W	575 W
Typical power draw	175 W	400 W

Safeguard instructions

For your protection, please read all these instructions regarding your appliance.

- **Read instructions**
Read and understand all the safety and operating instructions before operating the appliance.
- **Ventilation**
Vents on the front and rear and the fan opening on the back panel of the Symantec Clientless VPN Gateway 4400 Series provide ventilation for reliable product operation and to protect it from overheating. These openings must not be blocked or covered. This product should not be placed in an enclosure unless proper ventilation is provided.
- **Power cord**

Caution: The power-supply cord is used as the main disconnect device. Ensure that the socket outlet is located or installed near the equipment and is easily accessible.

Caution: Français: Le cordon d'alimentation sert d'interrupteur général. La prise de courant doit être située or installée à proximité du matériel et offrir un accès facile.

Caution: Deutsch: Zur sicheren Trennung des Gerätes vom Netz ist der Netzstecker zu ziehen. Vergewissern Sie sich, daß die Steckdose leicht zugänglich ist.

Warning: To reduce the risk of electrical shock, do not disassemble this product. Return it to Symantec when service or repair work is required. Opening or removing covers may expose you to dangerous voltage or other risks. Incorrect reassembly can cause electric shock when this product is subsequently used.

Note: Opening the cover voids your warranty!

Warning: To prevent a possible electrical shock when installing the device, ensure that the power cord for the device is unplugged before installing network cables.

Warning: To prevent a possible electrical shock, when adding the device to a system, disconnect all power cords, if possible, from the existing system before connecting the signal cable to that device.

Warning: To prevent a possible electrical shock during an electrical storm, do not connect or disconnect cables.

Warning: To prevent a possible electrical shock from touching two surfaces with different electrical grounds, use one hand, when possible, to connect or disconnect signal cables.

Warning: To avoid a shock hazard, the power cord must be connected to a properly wired and earthed receptacle.

Warning: To avoid a shock hazard, any equipment to which this product will be attached must also be connected to properly wired receptacles.

Warning: Electrical current from power, telephone, and network cables is hazardous.

■ Operating the unit in an equipment rack

If you plan to install the Symantec Gateway Security 4400 Series in an equipment rack, use these precautions:

- Ensure the ambient temperature around the appliance (which may be higher than the room temperature) are within the specified limits.
- Ensure there is sufficient air flow around the unit.
- Ensure electrical circuits are not overloaded; consider the nameplate ratings of all the connected equipment and ensure you have overcurrent protection.
- Ensure the equipment is properly grounded, particularly any equipment connected to a power strip.
- Do not place any objects on top of the appliance.

Product certifications

The Symantec Clientless VPN Gateway 4400 Series is designed to meet the following regulatory requirements for public safety:

- UL and CSA Standard for Safety of Information Technology Equipment including Electrical Business Equipment (UL 60950, 3rd Edition and CAN/CSA C22.2 No.60950-00). This Class A digital apparatus complies with Canadian ICES-003. (Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.)
- VCCI
- CE
- FCC part 15B, Class A
- EMC:
 - EN55022 (1998), Class A Emissions (Radiated & Conducted)
 - EN61000-3-2 (2000), Harmonics
 - EN61000-3-3 (1995), Flicker
 - EN61000-4-2 (1995), ESD: 8 kV AD, 4 kV CD
 - EN61000-4-3 (2002), RF Immunity: 10 V/m, 80 MHz - 1 GHz
 - EN61000-4-4 (1995), EFT/Burst: 1 kV Power, .5 kV Signal Cables
 - EN61000-4-5 (1995), Surge: 1 kV (L-L), 2 kV (L-G)
 - EN61000-4-6 (1996), Conducted RF Immunity: 3V, 150 kHz – 80 MHz
 - EN61000-4-11 (1994): >95%/0.5T, 30%/25T, >95%/250T
 - Safety:EN60950-1 (2002)

This device complies with Part 15B of the FCC Rules. Operation is subject to two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Index

Numerics

30-day grace period 39, 44, 52

A

access lists, checklists 66
activating, license files 44
additive licenses 51
address configuration 22
administrator password 23
advanced configurations 29
appliance setup 24
authentication method, checklist 60

B

back panel features model 4420 11, 13
browser support 6, 22

C

CD-ROMs, replacement 8
certifications 91
configuration
 setup worksheets 23
connecting
 model 4420 to network 12
 model 4460 to network 14
 SGMI 28
cooling fan 12, 14

D

displaying, system information 26
documentation, supplied 7

E

electric shock 89

F

factory reset 27

front panel controls
 description 19
 locking 29
front panel layout 19

G

GNU library general public license 80

H

high availability license bundles 53

I

inside interface, configuring 24
installing
 model 4420 power cord 13
 model 4460 power cord 14
 rack mount 10
 stand-alone 9
IP addresses checklist 63

L

LCD display 19
LEDs. See status indicators.
license certificates 51
License File Organization Worksheet 43
license files
 activating 44
 removing 50, 51
 uploading 50
license serial number
 obtaining 40
 organizing 40
license types 51
licensing
 collecting product and contact information 40
 explanation 51
 obtaining your license file 42
 organizing your license files 42
 planning for your license 41

- sorting your serial numbers 40
- load balancing license bundles 53

M

- maintenance
 - contracts 52
 - Gold Maintenance 52
 - renewals 53
- maintenance, Platinum support 53
- Microsoft Internet Explorer, version 6, 22
- model
 - 4420 11, 13
- monitoring mode 26
- Mounting 10

N

- navigation buttons 19
- Netscape, version 6, 22
- network
 - address information 22
 - architecture checklist 68
 - configuration 22
 - connections
 - model 4420 12
 - models 4400 14
 - setup 27
 - setup worksheet 23
 - password 23
 - status indicators 20

O

- obtaining, license file 27, 44
- operating system, restoring 36

P

- password
 - administrator 23
 - changing 24
 - LCD 23
 - logon 28
 - root password 23
- Platinum support 53
- power cord installation
 - model 4420 13
 - model 4460 14
- power reset switch 14
- power socket 12, 14

- power switch 12, 14
- product component list 7
- product specifications 88
- proxies checklist 64

R

- regulatory requirements 91
- removing license file 50, 51
- replacing, CD-ROMs 8
- reset 27
- restoring, operating system 36
- root password 23

S

- safety
 - electric shock 89
 - equipment rack 90
- Security Gateway Management Interface. See SGMI.
- security plan
 - checklist 56
 - worksheets 59
- serial console port 12, 14
- Serial Number Certificates, gathering 40
- setting up
 - appliance 24
 - SGMI 28
- SGMI
 - browser address 28
- shutdown 27
- site hardware information, checklist 61
- software serial number certificate 44
- status indicators
 - active connection 20
 - disk 20
 - Ethernet connection 20
 - hard disk drive 20
 - receive 20
 - temp 20
 - traffic 20
 - transmit 20
 - Web activity 20
- Symantec Software License Agreement 71
- Symantec System ID 40, 46
- Symantec System ID, defined 41
- system
 - information 26
- system menu
 - factory reset 27

- network setup 27
- shutdown 27
- system ID 27

T

- TCP/IP checklist 62
- temperature 20
- troubleshooting 86
- Turn 13
- turning on
 - model 4420 13
 - model 4460 15

U

- unlocking front panel controls 29
- USB port
 - modem connection 12, 14
- user documentation 7
- using locked front panel controls 29
- using, system menu 27

W

- WEB service, checklist 65
- WinRAR 41
- WinZip 41
- worksheets
 - network setup 23
 - security planning 59

